

UNITED STATES PATENT APPLICATION

of

Joel M. Soderberg

Brian J. Deen

and

Alexander I. Hopmann

for

**MAPPING CONNECTIONS AND
PROTOCOL-SPECIFIC RESOURCE IDENTIFIERS**

WORKMAN, NYDEGGER & SEELEY

A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

UNITED STATES PATENT APPLICATION

BACKGROUND OF THE INVENTION

1. The Field of the Invention

The present invention relates to mapping connections and protocol specific resource identifiers. More specifically, the present invention relates to a front-end server providing access to content stored on a back-end server by mapping the connection between a client system and the front-end server with the corresponding connection between the front-end server and the back-end server. As needed, protocol specific resource identifiers are generated to match the protocol associated with the connection between the client system and the front-end server.

2. Background and Related Art

At times, a client system on an insecure network, such as the Internet, may request hypertext transfer protocol ("HTTP") content from a back-end server that is operating on a relatively secure private network, such as a corporate intranet. It may also be the case that such HTTP requests made by the client are encrypted to prevent unwanted data interception. Conventionally, the back-end server would decrypt the request, processes the request, encrypt data associated with the request, and send the data to the client system. However, encrypting and decrypting HTTP data is computationally expensive and as result drains resources a back-end server might use to perform other functions, such as query a database or other configured tasks.

Where multiple back-end servers provide related content, a front-end server may be used as a common point of access. Client systems direct requests to the front-end server and the front-end server forwards the request to the appropriate back-end server. This allows for content to be distributed and enables load balancing across the servers where the

1 content is available. For example, email stores for an organization may be distributed over
2 several back-end servers, with a single front-end server allowing all stores to be accessed
3 using a single resource identifier, such as "http://www.company.com/email". When the
4 front-end server receives a request for email, the request is directed to the back-end server
5 where the corresponding email stored is located.

6 To prevent eavesdropping and insure data integrity, communication between the
7 client systems and the front-end server may use a secure protocol. In contrast, the
8 communication between the front-end server and the back-end server may not need to use
9 a secure protocol because the communication link itself may not subject to tampering, such
10 as a communication link that is isolated from external contact. However, using a secure
11 protocol between the client and front-end server with an insecure protocol between the
12 front-end server and back-end server leads to certain problems.

13 Consider for example, providing email using HTTP for communication between
14 the back-end server and the front-end server, and using HTTPS (HTTP with a secure
15 sockets layer or SSL) for the communication between the front-end server and the client
16 system. At login, the client system submits an HTTPS request to view the client system's
17 inbox. The front-end server receives the request, performs the appropriate decryption, and
18 directs the request to the back-end server where the inbox is located. In response, the
19 back-end server generates an HTTP version of the inbox (i.e., the uniform resource
20 locators ("URLs") for the inbox specify "http" as the protocol). The response is returned
21 to the front-end server and sent to the requesting client system. Upon selection of a URL,
22 the client system generates a request for the corresponding email. However, because the
23 URL specifies HTTP as the protocol, the request to the front-end server is made over an
24

1 insecure connection. Obviously, this is not what the client system intended since the client
2 system initiated contact using a secure protocol.

3 Moreover, requesting email content over an insecure connection is a further
4 problem because the front-end server may be configured to communicate over external
5 insecure networks only using protocols such as HTTPS. Thus, a front-end server may not
6 be configured to use insecure protocols on insecure networks. As a result, the front-end
7 server rejects any requests from the client that use an insecure protocol. Alternatively, the
8 front-end server may be configured to allow insecure requests for some data, such as
9 publicly accessible Web pages, while rejecting requests for more sensitive content, such as
10 email content. In either case, the potential exists for the front-end server to reject a request
11 submitted over an insecure connection.

12 Although communicating between the front-end server and the back-end server
13 with the same protocol that is used between the client system and the front-end server may
14 solve the HTTP URL problem, this approach is undesirable because it requires the back-
15 end server to encrypt the content it provides. As noted above, this encryption may be
16 computationally expensive and may serve no useful purpose if the connection between the
17 front-end server and the back-end server is not subject to attack. Furthermore, the front-
18 end server is required first to decrypt the content it receives from the back-end server,
19 using the key negotiated between the front-end server and the back-end server, and then to
20 re-encrypt the content, using the key negotiated between the front-end server and the
21 client. To avoid the unneeded encryption/decryption operations, the front-end server could
22 parse the content it receives from the back-end servers and modify protocol specific
23 resource identifiers as needed. However, similar to the extra encryption/decryption
24 processing, parsing content at the front-end server for protocol specific resource identifiers

1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

1 is computationally expensive and requires storing content, at least temporarily, on the
2 front-end server. For these reasons and others, parsing content at the front-end server is
3 also undesirable.

4 Therefore, systems, methods, and computer program products are desired for
5 mapping connections and protocol specific resource identifiers, where the systems,
6 methods, and computer program products impose minimal resource requirements on the
7 front-end server and back-end servers.

SUMMARY OF THE INVENTION

The principles of the present invention provide for mapping connections and protocol specific resource identifiers. When a front-end server receives a request that is ultimately directed to a back-end server, the front-end server performs certain operations on the request before forwarding it to the back-end server. First, the front-end server decrypts the request as needed. Second, the front-end inserts a protocol element into the request sent to the back-end server to notify the back-end server of the protocol used in the client's request to the front-end server. When the back-end server retrieves data associated with the request, the back-end server passes the content to the front-end server. When received, the front-end server sends the content to the client according to the protocol used in the client's request. The back-end server generates protocol specific resource identifiers within the content that are consistent with the protocol element or information included with the request for content, even though the front-end server and the back-end server may use another protocol in communicating with each other. For example, the client system and the front end server may communicate using HTTPS, while the front end server communicates with the back end server using HTTP.

Because the front-end server performs any needed encryption and decryption for requests only once, the resources of the front-end server and back-end servers are freed up to perform other tasks. Also, the front-end server will not reject subsequent requests for content that the client generates based on the selection of protocol specific resource identifiers in content that has been received. Because the back-end server generates resource identifiers consistent with the protocol used between the client system and the front-end server, requested content may be sent to the client system even where the front-end server and back-end server communicate using a protocol that is not entirely

1 compatible with communication protocol used between the client system and the front-end
2 server.

3 Additional features and advantages of the invention will be set forth in the
4 description which follows, and in part will be obvious from the description, or may be
5 learned by the practice of the invention. The features and advantages of the invention may
6 be realized and obtained by means of the instruments and combinations particularly
7 pointed out in the appended claims. These and other features of the present invention will
8 become more fully apparent from the following description and appended claims, or may
9 be learned by the practice of the invention as set forth hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to describe the manner in which the above recited and other advantages and features of the invention can be obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof, which is illustrated, in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

Figure 1 illustrates an exemplary system that provides a suitable operating environment for the present invention;

Figure 2 is illustrates a client system, front-end server, and back-end server operating in accordance with the present invention; and

Figures 3A and 3B are a flow diagram illustrating a method for mapping connections and protocol specific resource identifiers.

DETAILED DESCRIPTION OF THE INVENTION

The present invention extends to methods, systems, and computer program products for mapping connections and protocol specific resource identifiers. The embodiments of the present invention may comprise a special purpose or general-purpose computer including various computer hardware components, as discussed in greater detail below.

Embodiments within the scope of the present invention also include computer-readable media for carrying or having computer-executable instructions or data structures stored thereon. Such computer-readable media can be any available media, which can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code means in the form of computer-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a computer-readable medium. Thus, any such connection is properly termed a computer-readable medium. Combinations of the above should also be included within the scope of computer-readable media. Computer-executable instructions comprise, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions.

Figure 1 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the invention may be implemented. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by computers in network environments. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. The sequence of instructions implemented in a particular data structure or program module represents examples of corresponding acts for implementing the functions or steps described herein.

Those skilled in the art will appreciate that the invention may be practiced in network computing environments with many types of computer system configurations, including personal computers, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by local and remote processing devices that are linked (either by hardwired links, wireless links, or by a combination of hardwired or wireless links) through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

With reference to Figure 1, an exemplary system for implementing the invention includes a general-purpose computing device in the form of a conventional computer 120, including a processing unit 121, a system memory 122, and a system bus 123 that couples various system components including the system memory 122 to the processing unit 121. The system bus 123 may be any of several types of bus structures including a memory bus

1 or memory controller, a peripheral bus, and a local bus using any of a variety of bus
2 architectures. The system memory includes read only memory (ROM) 124 and random
3 access memory (RAM) 125. A basic input/output system (BIOS) 126, containing the basic
4 routines that help transfer information between elements within the computer 120, such as
5 during start-up, may be stored in ROM 124.

6 The computer 120 may also include a magnetic hard disk drive 127 for reading
7 from and writing to a magnetic hard disk 139, a magnetic disk drive 128 for reading from
8 or writing to a removable magnetic disk 129, and an optical disk drive 130 for reading
9 from or writing to removable optical disk 131 such as a CD-ROM or other optical media.
10 The magnetic hard disk drive 127, magnetic disk drive 128, and optical disk drive 130 are
11 connected to the system bus 123 by a hard disk drive interface 132, a magnetic disk drive-
12 interface 133, and an optical drive interface 134, respectively. The drives and their
13 associated computer-readable media provide nonvolatile storage of computer-executable
14 instructions, data structures, program modules and other data for the computer 120.
15 Although the exemplary environment described herein employs a magnetic hard disk 139,
16 a removable magnetic disk 129 and a removable optical disk 131, other types of computer
17 readable media for storing data can be used, including magnetic cassettes, flash memory
18 cards, digital versatile disks, Bernoulli cartridges, RAMs, ROMs, and the like.

19 Program code means comprising one or more program modules may be stored on
20 the hard disk 139, magnetic disk 129, optical disk 131, ROM 124 or RAM 125, including
21 an operating system 135, one or more application programs 136, other program modules
22 137, and program data 138. A user may enter commands and information into the
23 computer 120 through keyboard 140, pointing device 142, or other input devices (not
24 shown), such as a microphone, joy stick, game pad, satellite dish, scanner, or the like.

1 These and other input devices are often connected to the processing unit 121 through a
2 serial port interface 46 coupled to system bus 123. Alternatively, the input devices may be
3 connected by other interfaces, such as a parallel port, a game port or a universal serial bus
4 (USB). A monitor 147 or another display device is also connected to system bus 123 via
5 an interface, such as video adapter 148. In addition to the monitor, personal computers
6 typically include other peripheral output devices (not shown), such as speakers and
7 printers.

8 The computer 120 may operate in a networked environment using logical
9 connections to one or more remote computers, such as remote computers 149a and 149b.
10 Remote computers 149a and 149b may each be another personal computer, a server, a
11 router, a network PC, a peer device or other common network node, and typically include
12 many or all of the elements described above relative to the computer 120, although only
13 memory storage devices 150a and 150b and their associated application programs 136a and
14 136b have been illustrated in Figure 1. The logical connections depicted in Figure 1
15 include a local area network (LAN) 151 and a wide area network (WAN) 152 that are
16 presented here by way of example and not limitation. Such networking environments are
17 commonplace in office-wide or enterprise-wide computer networks, intranets and the
18 Internet.

19 When used in a LAN networking environment, the computer 120 is connected to
20 the local network 151 through a network interface or adapter 153. When used in a WAN
21 networking environment, the computer 120 may include a modem 154, a wireless link, or
22 other means for establishing communications over the wide area network 152, such as the
23 Internet. The modem 154, which may be internal or external, is connected to the system
24 bus 123 via the serial port interface 146. In a networked environment, program modules

1 depicted relative to the computer 120, or portions thereof, may be stored in the remote
2 memory storage device. It will be appreciated that the network connections shown are
3 exemplary and other means of establishing communications over wide area network 152
4 may be used.

5 In this description and in the following claims, the term "computer" should be
6 interpreted broadly to encompass a general purpose or special purpose computer or any
7 other computing device including, but not limited to, various computer hardware
8 components, such as those illustrated in Figure 1. A "computer system" may include a
9 group of one or more computers that interact cooperatively to perform one or more
10 functions. A "network system" may include a plurality of interconnected computer
11 systems, as well as other devices that may be connected to computer systems. A "client
12 system" may be a computer system, a group of computer systems, other devices that may
13 be associated with a network system, or some combination thereof, that use the services of
14 another computer system. In contrast, a "server system" may be a computer system, group
15 of computer systems, other devices that might be associated with a network system, or
16 some combination thereof, that provide services to another computer system.

17 Note that a computer system may use the services of another computer system and
18 yet still provide services to other computer systems. Thus, a client system in one context
19 may also be a server system in another context. Similarly, a server system in one context
20 may also be a client system in another context. This principle is applicable to all
21 embodiments of the present invention.

22 The HyperText Transfer Protocol, or HTTP, is the underlying protocol used by the
23 World Wide Web ("Web"). HTTP defines how messages are formatted and transmitted,
24

1 and what actions Web servers and browsers should take in response to various commands.
2 HTTP is an insecure protocol.

3 Secure Sockets Layer, or SSL, is a protocol developed for transmitting private
4 documents via the Internet. SSL works by simultaneously (at both a client system and a
5 server) generating a symmetric key from a private/public encryption key pair, and then
6 using the symmetric key to encrypt data that is transferred over the SSL connection. For
7 secure communication, SSL and HTTP may be used together.

8 As the term implies, a resource identifier uniquely identifies resources or content.
9 HTTP defines one type of resource identifier, a Uniform Resource Locator, or URL. A
10 Uniform Resource Locator is the global address of content, such as documents and other
11 resources available on the World Wide Web. The first part of the URL indicates the
12 protocol to use in requesting a resource. For example, if the first part of the URL is
13 "http:", the HTTP protocol is used. In contrast, if the first part of the URL is "https:", SSL
14 is used in connection with the HTTP protocol. The remainder of the URL specifies the IP
15 address or the domain name where the resource is located, including any necessary
16 directory hierarchy. Due to the close relationship between HTTPS and SSL, specifically
17 that one generally, but not necessarily, implies the other, HTTPS and SSL may be used
18 synonymously in various portions of the following disclosure.

19 While Figure 1 and the corresponding discussion above provide a general
20 description of a suitable environment in which the invention may be implemented, it will
21 be appreciated that the features of the present invention may be practiced in association
22 with a variety of configurations. Therefore, the components illustrated in Figure 2 provide
23 only one exemplary environment for practicing the present invention. It should be
24 understood that the present invention, as described in connection with Figure 2, may also

1 be practiced in a configuration that additionally includes one or more of the components as
2 shown in Figure 1.

3 Figure 2 illustrates a network configuration suitable for implementing the
4 principles of the present invention. The configuration includes client 200, insecure
5 network 230, front-end server 210, private network 240, and back-end servers 220. Back-
6 end servers 220 includes back-end server 220a, 220b, 220c and 220d respectively.
7 Although only one client and one front-end server are illustrated in Figure 2, the general
8 principles disclosed herein can be readily adapted to configurations having any number of
9 clients systems and front-end servers in combination.

10 The insecure network 230, which may comprise the Internet, includes client 200,
11 which is in communication with front-end server 210. Private network 240 includes the
12 back-end servers 220a, 220b, 220c and 220d, each of which is also in communication with
13 front-end server 210. Network configurations for private network 240 include, but are not
14 limited to, Ethernet, token ring, Arcnet, or any other network configuration or combination
15 thereof. Insecure network 230 can be any of these configurations, including the Internet.
16 Although described in the context of a client system on an insecure network
17 communicating with a back-end server on a secure network, the present invention is not
18 necessarily limited to any particular network or communication protocol. Likewise, the
19 present invention is not limited to requests for any particular type of content. Those of
20 skill in the art will recognize that a wide variety of content may be accessed through front-
21 end server 210, including email messages, financial information, sports data, technical
22 documents, databases, etc. Content, particularly content that is accessible over the World
23 Wide Web and referred to as Web content, often includes markups to improve the
24

1 content's display and/or scripts that may be executed. However, the present invention is
2 not necessarily limited to any particular type of content.

3 Front-end server 210 may prevent insecure communications from entering or
4 exiting private network 240 based on certain criteria. For example, front-end server 210
5 may prohibit any unencrypted HTTP requests from entering or exiting private network
6 240. Front-end server 210 may include encryption/decryption module 211 and HTTP
7 router module 212.

8 Encryption/decryption module 211 decrypts messages received from a client, such
9 as client 200, before forwarding them to a back-end server, such as back-end server 220c,
10 and may encrypt messages received from a back-end server before forwarding them to a
11 client. This may involve encryption or decryption operations to the content of an HTTP
12 request, including requests that use SSL. Encryption and decryption may be used to map
13 SSL connections to insecure connections or to map insecure connections to SSL
14 connections.

15 Communication between the devices illustrated in Figure 2 may take place using
16 different protocols and may take place on different ports. For instance, one port may be
17 configured for insecure connections using HTTP, while another may be configured for
18 secure connections using HTTPS. For example, insecure HTTP communications
19 conventionally occur over port 80 and secure HTTPS communications, ones that use SSL,
20 occur over port 443. When information is received at one of these ports the front-end
21 server processes the information consistent with the configuration of that port, insecure on
22 port 80 and secure on port 443. While the present invention is discussed in the context of
23 the exemplary configuration mentioned above, the invention is not limited to this
24 configuration. The present invention may be practiced in any configuration where there is

1 a client, a front-end server and one or more back-end servers, all of which may need to
2 communicate over one or more networks using one or more protocols.

3 HTTP router module 212 tracks information about HTTP content that is received
4 by front-end server 210. This tracking may include, which client requests were received
5 over a particular connection and which client requests were sent to which back-end servers.
6 If a request is received over an SSL connection, HTTP router module 212 adds a header to
7 the request before it is forwarded to a back-end server. The included header notifies the
8 back-end server that the original request was received over an SSL connection. Otherwise
9 the back-end server would not know that the front-end server received the request over a
10 secure SSL connection because the back-end server is aware only that it received the
11 request from the front-end server on an unencrypted port (port 80 in this case).

12 In operation, client 200 generates HTTP request 250 and sends it to front-end
13 server 210. The request, for example, may be for the email inbox associated with
14 client 200. Email inboxes often show the sender, subject, and relevant dates for emails that
15 have been received, including some type of indication whether or not a particular email has
16 been read. However, the present invention is not necessarily limited to requests for an
17 email inbox or any particular information being included within an email inbox. After
18 generation, the request is sent to port 443 of front-end server 210 as SSL request 251.
19 Encryption/decryption module 211 decrypts the request.

20 HTTP router module 212 includes information specifying the content that is
21 available on the various back-end servers 220. The HTTP router module 212 determines
22 that the request was an SSL request, adds a header to the request, and tracks that the
23 request is sent to back-end server 220c. The header may comprise a "Via:" or "User-
24 agent:" HTTP request header to indicate the request was received by front-end server 210

1 over an SSL connection and is being forwarded to back-end server 220c for processing.
2 However, the present invention is not necessarily limited to the use of any particular
3 header. Front-end server 210 then forwards the request and included header, as HTTP
4 request 252, to port 80 of back-end server 220c. In one example, the header is "Front-End-
5 HTTPS: on" and the header causes the back-end servers 220 to generate protocol specific
6 resource identifiers in the requested content that are consistent with the connection
7 between the client 200 and the front-end server 210.

8 The back-end server 220c processes the request and provides content that is
9 compatible with a secure connection. For example, back-end server 220c may generate
10 one or more protocol specific resource identifiers that are consistent with the SSL
11 connection between client 200 and front-end server 210. For an HTTP version of the
12 email inbox, this involves generating URLs that identify HTTPS as the protocol to be used
13 in making requests for individual emails. Without the header that was included with the
14 request, back-end server 220c would generate URLs that identify HTTP as the protocol to
15 be used in making requests for individual emails because the request was received at port
16 80, the default HTTP port. If the appropriate protocol specific resource identifiers are not
17 generated, then future client requests that originate from the protocol specific resource
18 identifiers included in the returned content will fail. More specifically, the front-end server
19 210 may be configured to prohibit any unencrypted HTTP requests from entering or
20 exiting the private network 240. The client 200 therefore communicates with the front-end
21 server 210 using HTTPS, which sends client requests to port 443. If the URLs included in
22 the content returned by the back-end servers 220 are HTTP URLs, then the client, upon
23 selecting those URLs from the returned content, will attempt to use port 80 instead of port
24 443. A request to port 80 will fail because the front-end server will only accept secure

1 requests to port 443. The present invention, by altering the URLs to conform with the
2 protocol used between the client 200 and the front-end server 210, ensures that the client
3 200 makes requests using the appropriate protocol specific resource identifiers.

4 Next, a response is sent back to the front end server 210, as HTTP response 253. Front-
5 end server 210 receives the response and HTTP router module 212 determines that the
6 response generated by back-end server 220c was the result of an SSL request from client
7 200. The response is encrypted by encryption/decryption module 211 and sent to client
8 200 as SSL response 254. The client receives SSL response 254 and views the requested
9 data. If the client system selects one of the URLs, such as an individual email appearing in
10 the inbox, client 200 generates an SSL request to front-end server 210 because the URL
11 identifies HTTPS as the protocol to be used in making a request for the URL's content.
12 Front-end server 210 maps the SSL request to an HTTP request and directs the request to
13 the appropriate back-end server. Most likely, the email contents will be stored at the same
14 back-end server providing the inbox content, so the HTTP request will be forwarded to
15 back-end server 220c. Back-end server 220c generates an HTTP version of the email
16 content, but uses HTTPS as the protocol identifier for any URLs within the content, and
17 sends the content to front-end server 210 as a response to the request for the email content
18 that front-end server 210 made for client 200. Upon receiving the requested content, front-
19 end server 210 performs the necessary processing for mapping the HTTP response to an
20 SSL response. Front-end server 210 then sends the SSL response to client 200.

21 The operation of the components in Figure 2 conserves the resources of the back-
22 end server 220c and front-end server 210 because encryption and decryption may be
23 performed only once at the front-end server 210. Furthermore, client 200 may request
24 resources based on resource identifiers provided by a back-end servers 220, without regard

1 to any differences in protocols for communicating between the client 200 and the front-end
2 server 210 and protocols for communicating between the front-end server 210 and the
3 back-end servers 220.

4 The operation of the components shown Figure 2 will now be described with
5 respect to Figures 3A and 3B, which are a flow diagram illustrating a method for mapping
6 connections and protocol specific resource identifiers. A step for communicating (310a)
7 with a client system includes the act of receiving a request (312) for content from the client
8 system. A front-end server receives the request in accordance with the communication
9 protocol used to exchange data between the client system and the front-end server. To
10 insure privacy and data integrity, the communication protocol may comprise a secure
11 protocol, such as SSL. However, a wide variety of secure protocols are known to those of
12 skill in the art and the present invention is not necessarily limited to any particular protocol
13 for communication between the front-end server and the client system. Other acts
14 associated with the step for communicating (310a) will be described below, with regard to
15 reference 310b.

16 A step for mapping (320a) communication between the client system and the front-
17 end server, to communication between the front-end server and a back-end server, may
18 include the act of decrypting (322) content received from the client if the communication
19 between the client system and the front-end server is encrypted. For example, if the client
20 is submitting a username and password with a request, the username and password may be
21 encrypted. The details of what content is encrypted generally depends on the particular
22 protocol used for secure communication. Therefore, both the act of decrypting (322)
23 content and the act of encrypting content (328) should be interpreted to include all or any
24 portion of the content, as may be appropriate for a particular protocol.

1 The step for mapping (320a) also may include an act of identifying (324) the back-
2 end server where the requested content is available and an act of adding (326) protocol
3 information to the request. The protocol information identifies the communication
4 protocol between the front-end server and the client system. Although not shown, an act of
5 tracking information associated with the client system's request for content may occur
6 during the mapping step as well. This information may include, for example, an identifier
7 for the connection between the client system and the front-end server and an identifier for
8 the connection between the front-end server and the identified back-end server so that
9 content received from the back-end server may be passed on to the client system using the
10 appropriate connection. Other acts associated with the step for mapping (320a) will be
11 described below, with regard to reference 320b.

12 A step for communicating (330) with the back-end server includes the acts of
13 sending (322) the request to the back-end server and receiving (334) a response from the
14 back-end server. Because the communication path between the front-end server and the
15 back-end server may be isolated from external contact, and therefore protected from
16 outside tampering, the protocol used for communication between the front-end server and
17 the back-end server need not be a secure protocol. The present invention does not require
18 the protocol used in communication between the front-end server and the client system to
19 be the same as the protocol used in communication between the front-end server and the
20 back-end server. Stated more generally, a communication protocol may be selected for
21 one connection, without regard for the communication protocol selected for the other
22 connection.

23 The content received from the back-end server may include one or more protocol
24 specific resource identifiers. However, these protocol specific resource identifies are based

1 on the protocol information, included with the request for content, that identify the
2 protocol used for communicating between the front-end server and the client system. This
3 allows the back-end server to account for protocol differences between how the front-end
4 server communicates with the client system and how the front-end server communicates
5 with the back-end server. For example, as described above, the front-end server may
6 communicate with the client system using a secure communication protocol, such as SSL,
7 and may communicate with the back-end server using an insecure protocol, such as HTTP.
8 Uniform resource locators for HTTP begin with "http:" and uniform resource locators for
9 HTTP implemented on top of SSL begin with "https:". If the back-end server generates
10 resource identifiers based on HTTP, then the resource identifiers in the content will not be
11 valid at the client system because the client system communicates with the front-end server
12 over a secure connection using SSL. In other words, the resource identifiers should
13 indicate HTTPS as the protocol for requesting content associated with the resource
14 identifiers. By identifying to the back-end server, the protocol used to communicate
15 between the front-end server and the client system, the back-end server is able to generate
16 resource identifiers that are appropriate for subsequent requests that may be made from the
17 client system.

18 Returning now to the step for mapping (320a and 320b) and the step for
19 communicating (310a and 310b), further acts that may be included within these steps will
20 be described. The step for mapping (320b) includes an act of encrypting content if the
21 protocol for communicating between the front-end server and the client system so requires,
22 and an act of sending (314) the response to the client system may be part of the step for
23 communicating (310b) with the client system.
24

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes, which come within the meaning and range of equivalency of the claims, are to be embraced within their scope.

What is claimed and desired secured by United States Letters Patent is: